

Information Technology Security

<u>Job Code</u>	<u>Class Title</u>	<u>Pay Grade</u>	<u>DEFAULT CODES</u>	
			<u>Supervisory</u>	<u>FLSA</u>
	IT Security Analyst I	30	N	N
	IT Security Analyst II	32	N	E
	IT Security Analyst II	34	N	E

OCCUPATIONAL CONCEPT

Plan, coordinate and implement security measures for information systems to regulate access to computer data files and prevent unauthorized modification, destruction, or disclosure of information.

TASKS

- Confer with users to discuss issues such as computer data access needs, security violations, and security related requirements of programming changes.
- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Document computer security and emergency measures, policies, procedures, and tests.
- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.
- Modify computer security files to incorporate new software, correct errors, or change individual access status.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Monitor use of data files and regulate access to safeguard information in computer files.
- Perform risk assessments and execute tests of information technology systems to ensure function and continuity of business computer related programs and activities and security measures.
- Review violations of computer security procedures and discuss with management.
- Coordinate implementation of the computer security system plan.
- Research security and disaster recovery information technologies of potential benefit to the organization.
- Identify and document the projected costs and benefits of information security technology capabilities.
- Coordinate or conduct security related systems training for users and organizational management

LEVELS OF WORK

IT Security Analyst I: This is entry level specialized technical work providing basic security and disaster recovery for information technology systems. This position will assist in implementing, monitoring and maintaining information technology security and disaster recovery policies and procedures, assist in maintaining security software applications, grant basic access to users, and assist users with non-complex security requirements. Incumbents typically have network/server security experience, security related applications experience, or business user experience in contingency planning. Tasks are varied but of a standardized nature, and performed under immediate supervision.

Minimum Requirements: Successful completion of 12 hours in computer science coursework or certification and six months experience in providing security and disaster recovery for information technology systems. Education may be substituted for experience as determined by the agency. Individual positions may require additional specific education and/or experience.

IT Security Analyst II: This is specialized technical work providing security and disaster recovery for information technology systems. Incumbents will implement, monitor and maintain information technology security and disaster recovery policies and procedures; researches, selects, modifies and maintains security software applications, provides technical assistance to users to resolve security problems, assists users with security requirements, grants access to users, and maintains documentation regarding the software security systems and disaster recovery. Tasks are varied involving several steps and require analytic thought. Assignments are given with general objectives for the desired outcome and incumbent has moderate latitude in establishing priorities and procedures. Work is outcome-oriented with progress reported periodically.

Minimum Requirements: Bachelor's degree in computer science or related field and two years experience or four years experience providing security and disaster recovery for information technology systems. Education may be substituted for experience as determined by the agency. Individual positions may require additional specific education and/or experience.

IT Security Analyst III: This is advanced specialized work functioning as the senior level information technology security officer. Responsible for the strategic planning, development, implementation and maintenance of information technology security programs and policies to ensure security for information technology resources including data, applications programs, system software, information technology equipment, services and physical access to facilities for an organization. Incumbents may serve as first line supervisors to lower level security staff. Incumbents are responsible for judging the value and importance of resources, establishing the proper risk classification for each resource and specifying the protections controls, monitoring security systems, policies, and procedures for compliance, authorizing access and assigning custody, administering organization specific business and resource protection controls for information, information technology resources and access, providing physical security for the data center and for information technology resources, and providing technical assistance in the selection, installation and implementation of security related hardware and software tools.

Minimum Requirements: Bachelor's degree in computer science or related field and three years experience or five years experience providing security and disaster recovery for information technology systems. Education may be substituted for experience as determined by the agency. Individual positions may require additional specific education and/or experience.

Necessary Special Requirements

Some positions in this class series may require a Kansas Bureau of Investigation Level 1 Security clearance at the time of appointment.